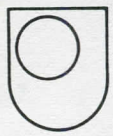
M335 NT HB

THE OPEN UNIVERSITY
Mathematics: A Third Level Course
M335 Studies in Pure Mathematics

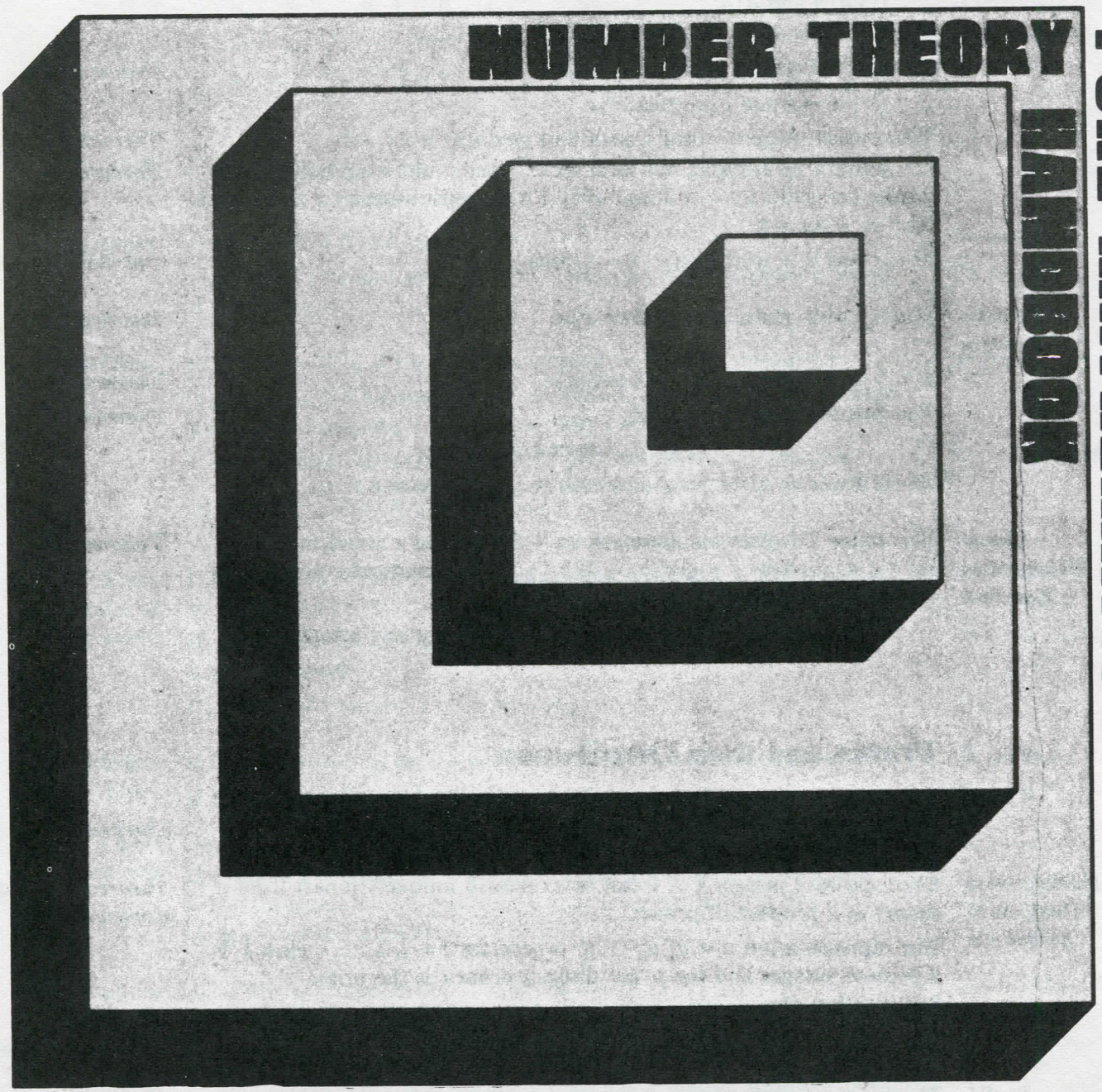


Note that you may take this handbook into the examination at the end of the course, provided you have not made any written additions to it, other than corrections.

STUDIES IN PURE MATHEMATICS

NUMBER THEORY

HANDBOOK



Copyright © 1981 The Open University

SUP 07602 3

Unit 1 Basic Ideas

Binomial Theorem

For any positive integer n,

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n, \quad \textbf{B } \textit{page 11}$$

where the binomial coefficient $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ for $0 \leqslant k \leqslant n$.

Division Algorithm

Given integers a and b, with $b > 0$, there exist unique integers q and r such that *Theorem 2-1*

$$a = qb + r, \quad 0 \leqslant r < b.$$

Greatest Common Divisor

Let a and b be integers, at least one of which is not zero. Then $\gcd(a,b)$ is the positive integer d satisfying *Definition 2-2*

(1) $d \mid a$ and $d \mid b$;
(2) if $c \mid a$ and $c \mid b$, then $c \leqslant d$.

(2) can be replaced by: *Theorem 2-6*

(2′) if $c \mid a$ and $c \mid b$, then $c \mid d$.

There exist integers x and y such that $\gcd(a,b) = ax + by$. *Theorem 2-3*

Let a and b be integers, not both zero. Then a and b are relatively prime (i.e. $\gcd(a,b) = 1$) if and only if there exist integers x and y such that $ax + by = 1$. *Theorem 2-4*

If $a \mid c$ and $b \mid c$, with $\gcd(a,b) = 1$, then $ab \mid c$. *Corollary 2*

Euclid's Lemma

If $a \mid bc$, with $\gcd(a,b) = 1$, then $a \mid c$. *Theorem 2-5*

If $k > 0$, then $\gcd(ka, kb) = k\gcd(a,b)$. *Theorem 2-7*

For positive integers a and b, *Theorem 2-8*

$$\gcd(a,b)\,\mathrm{lcm}(a,b) = ab,$$

where $\mathrm{lcm}(a,b)$ is the least common multiple of a and b.

Linear Diophantine Equation

The linear Diophantine equation $ax + by = c$ has a solution if and only if $d \mid c$, where $d = \gcd(a,b)$. If x_0, y_0 is any particular solution of this equation then all others are given by *Theorem 2-9*

$$\{x = x_0 + (b/d)t, \quad y = y_0 - (a/d)t, \quad t \text{ any integer.}\}$$

Unit 2 Primes and their Distribution

If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$. *Theorem 3-1*

Fundamental Theorem of Arithmetic

Every positive integer $n > 1$ can be expressed uniquely (apart from order) as a product of primes. *Theorem 3-2 and Corollary*

The representation $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ where, for $i = 1, 2, \ldots, r$, each k_i is a positive integer and the p_i are distinct primes, is the prime factorization of n.

If $p_1 < p_2 \ldots < p_r$ the factorization is in canonical form.

Euclid

There are infinitely many primes. *Theorem 3-4*

Dirichlet

If a and b are relatively prime positive integers, then a, $a + b$, $a + 2b$, $a + 3b, \ldots$ contains infinitely many primes. [Proof given only for particular cases.] — *Theorem 3-7*

$a > 1$ is an nth power if and only if in the prime factorization of a all the exponents are divisible by n. — *SAQ 4*

If $c > 1$ is not the nth power of an integer, then $\sqrt[n]{c}$ is not a rational number. — *SAQ 7*

Goldbach Conjecture

Every even positive integer is the sum of two numbers that are either primes or 1. [No proof or refutation known.] — **B** *page 58*

Fibonacci Sequence

The Fibonacci sequence is defined by — **B** *page 287*

$$u_1 = u_2 = 1, \quad u_n = u_{n-1} + u_{n-2} \quad \text{for } n \geqslant 3.$$

($u_0 = 0$, if convenient.)

Properties:

$\gcd(u_n, u_{n+1}) = 1$; — *Theorem 13-1*

$u_{m+n} = u_{m-1}u_n + u_m u_{n+1}$; — **B** *page 289*

$\gcd(u_m, u_n) = u_d$ where $d = \gcd(m, n)$; — *Theorem 13-3*

$u_m \mid u_n$ if and only if $m \mid n$, for $m > 2$. — *Corollary*

Unit 3 Congruence

Congruence

$a \equiv b \pmod{n}$ if and only if $n \mid a - b$. — *Definition 4-1*

$a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n. — *Theorem 4-1*

Definitions

$\{0, 1, 2, \ldots, n-1\}$ is the set of least positive residues modulo n. — **B** *page 71*

$\{a_1, a_2, \ldots, a_n\}$ is a complete set of residues modulo n if every integer is congruent modulo n to one and only one of the a_k.

The set of least absolute residues is the complete set of residues satisfying $-\frac{n}{2} < a_k \leqslant \frac{n}{2}$ for $k = 1, 2, \ldots, n$. — *Unit 3, page 46*

Some Properties of Congruence

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$. — *Theorem 4-2*

If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, where $\gcd(m, n) = 1$, then $a \equiv b \pmod{mn}$. — *Theorem, Unit 3, page 47*

If a is an odd integer, $a^2 \equiv 1 \pmod{8}$. — *SAQ 6*

Cancellation Laws

If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$. — *Theorem 4-3*

If $ca \equiv cb \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$. — *Corollary*

Linear Congruences

The linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d \mid b$, where $d = \gcd(a, n)$. If $d \mid b$ then it has d mutually incongruent solutions modulo n. If $\gcd(a, n) = 1$ then $ax \equiv b \pmod{n}$ has a unique solution modulo n. — *Theorem 4-7*, *Corollary*

Strategy for solving the linear congruence $ax \equiv b \pmod{n}$

1. For a solution, check that $\gcd(a, n) \mid b$. — *Tape Section 3.5*
2. Cancel all common divisors of a, b and n.
3. Cancel all remaining common divisors of a and b. The resulting congruence, $a'x \equiv b' \pmod{n'}$, then has a unique solution modulo n'.

4. Replace a' or b' by any convenient number to which it is congruent modulo n'.
5. Multiply through the congruence by any convenient number which is relatively prime to n'.

Chinese Remainder Theorem Let $n_1, n_2, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$$x \equiv a_1 (\mathrm{mod}\, n_1),\ x \equiv a_2 (\mathrm{mod}\, n_2), \ldots, x \equiv a_r (\mathrm{mod}\, n_r)$$

has a simultaneous solution, which is unique modulo $n_1 n_2 \ldots n_r$. *Theorem 4-8*

Unit 4 Fermat's Theorem

Fermat's Little Theorem If p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$. *Theorem 5-1*

Corollary If p is prime, then $a^p \equiv a \pmod{p}$ for any integer a.

Wilson's Theorem If p is prime, then $(p-1)! \equiv -1 (\mathrm{mod}\, p)$. *Theorem 5-2*

The quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$, where p is an odd prime, has a solution if and only if $p \equiv 1 \pmod{4}$. *Theorem 5-3*

Polynomial Congruence A polynomial congruence is an expression

$$P(x) = a_r x^r + a_{r-1} x^{r-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{n}$$

where P is an integral polynomial (i.e. a polynomial with integer coefficients). The degree of the polynomial is the highest exponent in P whose coefficient is not congruent to 0 modulo n.

Lagrange's Theorem If p is a prime and

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \not\equiv 0 \pmod{p}$$

is a polynomial of degree $n \geqslant 1$ with integral coefficients, then the congruence

$$f(x) \equiv 0 (\mathrm{mod}\, p)$$

has at most n incongruent solutions modulo p. *Theorem 8-5*

Corollary If p is prime and $d \mid n - 1$, then the congruence

$$x^d - 1 \equiv 0 (\mathrm{mod}\, p)$$

has exactly d solutions.

Unit 5 Multiplicative Functions

$\tau(n)$ = the number of positive divisors of $n = \sum_{d \mid n} 1$. *Definition 6-1*

$\sigma(n)$ = the sum of the positive divisors of $n = \sum_{d \mid n} d$.

Euler's Phi Function $\phi(n)$ = the number of positive integers not exceeding n which are relatively prime to n. *Definition 7-1*

τ, σ and ϕ are multiplicative functions. (A number-theoretic function f is multiplicative if $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$.) *Theorems 6-3 and 7-2*

If $n = p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$ is the prime factorization of $n > 1$, then the positive divisors of n are precisely those integers d of the form

$$d = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r} \quad \text{where } 0 \leqslant \alpha_i \leqslant k_i\ (i = 1, 2, \dots, r).$$

Theorem 6-1

Formulae for τ, σ and ϕ

$$\tau(n) = (k_1 + 1)(k_2 + 1)\dots(k_r + 1)$$

Theorem 6-2

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1}\,\frac{p_2^{k_2+1} - 1}{p_2 - 1}\cdots\frac{p_r^{k_r+1} - 1}{p_r - 1}$$

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)$$

Theorem 7-3

If f is a multiplicative function, then so also is F defined by

$$F(n) = \sum_{d|n} f(d).$$

Theorem 6-4

Useful Technique

As d runs through the divisors of n so does n/d.

Euler's Theorem

If n is a positive integer and $\gcd(a, n) = 1$ then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Theorem 7-5

Greatest Integer Function

$[x]$ is the largest integer less than or equal to x (for any real x). Any real x can be written uniquely as

$$x = [x] + \theta \quad \text{where } 0 \leqslant \theta < 1.$$

Definition 6-4

If n is a positive integer and p is a prime, then the exponent of the highest power of p that divides $n!$ is $\sum_{k=1}^{\infty} [n/p^k]$.

Theorem 6-9

Unit 6 The Quadratic Reciprocity Law

Legendre Symbol

If p is an odd prime and $\gcd(a, p) = 1$, then

$$(a/p) = \begin{cases} +1 \text{ if } a \text{ is a quadratic residue of } p, \\ -1 \text{ if } a \text{ is a quadratic nonresidue of } p. \end{cases}$$

Definition 9-2

The quadratic residues of p, an odd prime, are congruent modulo p to $1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2$.

SAQ 2

Euler's Criterion

Let p be an odd prime and $\gcd(a, p) = 1$. Then a is a quadratic residue or nonresidue of p according as, respectively,

$$a^{(p-1)/2} \equiv 1 \pmod{p} \quad \text{or} \quad a^{(p-1)/2} \equiv -1 \pmod{p}.$$

Theorem 9-1 Corollary

Properties of the Legendre Symbol

Let p be an odd prime and a and b be integers which are relatively prime to p. Then:

(1) if $a \equiv b \pmod{p}$, then $(a/p) = (b/p)$;
(2) $(a^2/p) = 1$;
(3) $(a/p) \equiv a^{(p-1)/2} \pmod{p}$;
(4) $(ab/p) = (a/p)(b/p)$;
(5) $(1/p) = 1$ and $(-1/p) = (-1)^{(p-1)/2}$.

Theorem 9-2

$$(2/p) = \begin{cases} 1 \text{ if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \\ -1 \text{ if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8. \end{cases}$$

Theorem 9-6

Gauss' Lemma

Let p be an odd prime and let $\gcd(a, p) = 1$. If n denotes the number of integers in the set

$$S = \left\{a, 2a, 3a, \dots, \left(\frac{p-1}{2}\right)a\right\}$$

whose remainders upon division by p exceed $p/2$ then $(a/p) = (-1)^n$.

Theorem 9-5

Gauss' Quadratic Reciprocity Law

If p and q are distinct odd primes, then

$$(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}.$$

That is $(p/q) = (q/p)$ if either $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, whilst $(p/q) = -(q/p)$ if $p \equiv q \equiv 3 \pmod 4$.

Unit 7 Continued Fractions

Notation and Basic Results

Let $[a_0; a_1, a_2, a_3, \ldots]$ be the (finite or infinite) continued fraction with partial denominators $(a_0), a_1, a_2, a_3 \ldots$. Define

$$\begin{aligned} p_0 &= a_0 & q_0 &= 1 \\ p_1 &= a_1 a_0 + 1 & q_1 &= a_1 \\ p_k &= a_k p_{k-1} + p_{k-2} & q_k &= a_k q_{k-1} + q_{k-2} \quad \text{for } k = 2, 3, \ldots . \end{aligned}$$

Then $p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}$, *Theorem 13-7*

and p_k and q_k are relatively prime, $k = 1, 2, 3, \ldots$. *Corollary*

The kth convergent C_k is defined to be $[a_0; a_1, a_2, \ldots, a_k]$ for $k = 1, 2, 3, \ldots$, and C_0 is a_0. Then: *Definition 13-2*

(1) $C_k = p_k/q_k$, $k = 0, 1, 2, \ldots$; *Theorem 13-6*

(2) $C_0 < C_2 < C_4 < \cdots$, $C_1 > C_3 > C_5 > \cdots$, and every convergent with an odd subscript is greater than every convergent with an even subscript. *Theorem 13-8*

Rational Numbers

Any rational number can be written (in exactly two ways) as a finite continued fraction, and, conversely, every finite continued fraction is rational. *Theorem 13-5 and* **B** *page 300*

Irrational Numbers

The value of any infinite continued fraction is an irrational number, and, conversely, every irrational number has a unique representation as an infinite continued fraction. *Theorem 13-9 and Theorem 13-11*

Any periodic continued fraction is a quadratic irrational and, conversely, any quadratic irrational has a periodic continued fraction. *Theorem, Unit 7, page 64*

Rational Approximations

If p_n/q_n is the nth convergent to the irrational number x, then *Corollary to Theorem 13-11*

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_{n+1} q_n} < \frac{1}{q_n^2}.$$

If $1 \leqslant b \leqslant q_n$, where p_n/q_n is the nth convergent to the irrational number x, and a and b are integers, then *Theorem 13-12*

$$\left| x - \frac{p_n}{q_n} \right| \leqslant \left| x - \frac{a}{b} \right|.$$

Let x be an irrational number. If the rational number a/b, where $b \geqslant 1$ and $\gcd(a, b) = 1$, satisfies *Theorem 13-13*

$$\left| x - \frac{a}{b} \right| < \frac{1}{2b^2},$$

then a/b is one of the convergents in the continued fraction representation of x.

Unit 8 Diophantine Equations

Pell's Equation

$x^2 - dy^2 = 1$, where d is a non-square positive integer.
Let p_k/q_k be the convergents of the continued fraction expansion of $\sqrt{d}$ and n be the length of the period of the expansion.

Theorem 13-16

(1) If n is even, then all positive solutions of $x^2 - dy^2 = 1$ are given by

$$x = p_{kn-1}, \quad y = q_{kn-1} \quad (k = 1, 2, 3, \ldots).$$

(2) If n is odd, then all the positive solutions of $x^2 - dy^2 = 1$ are given by

$$x = p_{2kn-1}, \quad y = q_{2kn-1} \quad (k = 1, 2, 3, \ldots).$$

Pythagorean Equation

All the primitive solutions (i.e. those solutions x, y, z of positive integers with $\gcd(x, y, z) = 1$ and x even—Lemma 1, **B** page 243) of the Pythagorean Equation $x^2 + y^2 = z^2$ are given by $x = 2st$, $y = s^2 - t^2$, $z = s^2 + t^2$ for integers $s > t > 0$ such that $\gcd(s, t) = 1$ and $s \not\equiv t \pmod 2$.

Theorem 11-1

Fermat's Conjecture (Last Theorem)

The Diophantine equation $x^n + y^n = z^n$ has no solution in positive integers x, y, z for n an integer greater than 2. [No proof or refutation known.]

The Diophantine equation $x^4 + y^4 = z^2$ has no solution in positive integers x, y, z.

Theorem 11-3

Sums of Squares

If m and n are each the sum of two squares, then so is their product:

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

Lemma, **B** *page 262*

A positive integer n is representable as the sum of two squares if and only if each of its prime factors of the form $4k + 3$ occur to an even power.

Corollary to Theorem 12-3

No positive integer of the form $4^n(8m + 7)$ can be represented as a sum of three squares. All others can.

Theorem 12-5

Lagrange

Any positive integer n can be written as the sum of four squares (some of which may be zero).

Unit 8, page 84

Glossary

Fermat number A Fermat number is an integer of the form $F_n = 2^{2^n} + 1$, where n is a positive integer. If F_n is prime, it is called a Fermat prime.

Mersenne number A Mersenne number is an integer of the form $M_n = 2^n - 1$, where n is a positive integer. If M_n is prime, it is called a Mersenne prime.

Perfect number A positive integer n is a perfect number if it is equal to the sum of all its positive divisors other than itself, i.e. if $\sigma(n) = 2n$.

Place value notation If N is written in the form

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0,$$

where b is a positive integer, $a_m \neq 0$ and $0 \leqslant a_k < b$ for $k = 0, 1, 2, \ldots, m$, then the base b place value notation for N is

$$N = (a_m a_{m-1} \ldots a_1 a_0)_b.$$

Quadratic irrational A quadratic irrational is a number of the form $r + s\sqrt{d}$, where r and s are rational numbers and d is a non-square positive integer.

Square-free An integer is square-free if it is not divisible by the square of any integer greater than 1.

Triangular number A positive integer n is triangular if it can be written in the form $n = \frac{1}{2}k(k + 1)$, where k is a positive integer.

Twin primes If p and $p + 2$ are both prime, they are called twin primes.

Printed in The United Kingdom
by The Open University